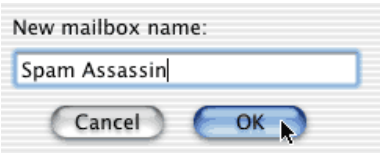
http://clx.asso.fr/spip/?Le-filtrage-de-spam-sous-Debian

POURRIEL

Le filtrage de spam sous Debian GNU/Linux

- Documentations - Technique -



Date de mise en ligne : mercredi 24 juillet 2002

Copyright © Club LinuX Nord-Pas de Calais - Tous droits réservés

Les e-mails non sollicités (*SPAM*, ou encore *POURRIEL*) envahissent réguliÚrement vos boîtes à lettres électroniques ? Une seule solution : installez un systÚme de filtrage tel que Spamassassin.

Le spam nous pourrit la vie, au moins autant que les 3 tonnes et demie de prospectus qu'on recoit chaque jour dans notre boîte aux lettres. Quoi de plus rageant que de mettre 10 minutes à récupérer 5 messages lorsque ces derniers se révèlent être du spam ?
Il existe des outils adaptés au filtrage des mails. Spamassassin en est un.

Packages nécessaires :

spamassassin, *procmail*, *fetchmail*, *qpopper* et votre MTA préféré (sous Debian celui par défaut est *exim*, je lui préfère *sendmail*, mais les goûts et les couleurs...).

Premier truc, installer tout ce joyeux bazar...

```
su -
```

on passe en root

```
apt-get install spamassassin procmail fetchmail qpopper exit
```

on quitte le root, c'est pas *secure* du tout

On va d'abord configurer fetchmail, pour aller récupérer les mails sur les serveurs de notre FAI ou de n'importe qui d'autre.

Configuration de Fetchmail

Sous Debian, on a la possibilité de lancer fetchmail en tant que root (beurk) ou d'un utilisateur lambda créé pour l'occasion, fetchmail (quelle originalité :))

J'ai passé la nuit à essayer de faire fonctionner fetchmail en non-root, puis j'ai abandonné, parce que vraiment... Je ne comprenais pas.

Donc, j'ai modifié le fichier `/etc/init.d/fetchmail` de cette manière :

```
OPTIONS="--daemon 30 --syslog"
```

J'ai supprimé les fonctions testconfig et fixconfperms, qui ne me servaient plus à rien

Et j'ai remplacé :
– Dans la section "start" du script, la ligne :

```
if start-stop-daemon ${START} \          "--command=${DAEMON} ${OPTIONS}" ${RUNUSER} <&- >/dev/null 2>&1
```

par

```
if $DAEMON ${OPTIONS} then;
```

– Dans la section "stop", la ligne :

```
if su "--command=${DAEMON} --quit" ${RUNUSER} <&- >/dev/null 2>&1
```

par

```
if kill $(pidof fetchmail) >/dev/null 2>&1 ; then                echo "fetchmail."
```

Ensuite, dans le fichier `/etc/fetchmailrc`, nécessaire au fonctionnement de Fetchmail à l'échelle du système (et non pas d'un utilisateur), j'ai saisi :

```
poll serveur.fai.tld protocol pop3          username "utilisateur" pass "xxxxxx" is "user-unix" here
```

Diverses options sont disponibles, comme `keep`, qui permet de garder une copie du message sur le serveur (attention, certains FAI apprécient modérément ça, et si, sur le serveur, la boîtes aux lettres dépasse une certaine taille (entre 5 et 20 Mo), ils bloquent la réception de nouveaux messages.

Il faut veiller à établir les bons droits sur ce fichier (`/etc/fetchmailrc`). En effet, ça ne serait pas très intelligent d'autoriser tout le monde à lire ce fichier, qui contient les mots de passe de vos messageries électroniques en clair :))

donc

```
chown root.root /etc/fetchmailrc chmod 0600 /etc/fetchmailrc
```

Depuis ce moment, votre machine interroge toutes les 30 secondes votre serveur pop (ça peut paraître rapide mais avec certaines mailing-list c'est obligatoire si on ne veut pas récupérer 800 mails en une fois), et envoie ces messages dans les comptes des utilisateurs.

Maintenant, on va configurer Procmail pour utiliser spamassassin, qui est l'objet de cet article :p

Configuration de Procmail

Première chose, pour les utilisateurs de sendmail, il faut ajouter procmail dans la liste des programmes utilisables par smrsh...

Pour ce faire :

```
ln -s /usr/bin/procmail /etc/mail/smrsh/procmail
```

Ensuite, créez dans le répertoire de l'utilisateur un fichier `.procmailrc`, contenant les "recipes" (ou règles) suivantes :

```
PMDIR=$HOME/Procmail LOGFILE=$PMDIR/log MAILDIR=$HOME/Maildir  :0fw | spamassassin -P  :0: * ^X-Spam-Status:
Yes spambox
```

La première recipe consiste à passer tous les messages à la moulinette de Spamassassin, la seconde à mettre tous

les messages considérés comme étant du spam dans un fichier à part, en l'occurence spambox.

Ensuite, il faut dire au MTA de passer par Procmail pour distribuer les mails... C'est le rôle du fichier `.forward` (toujours dans le répertoire utilisateur), qui doit contenir :

```
"| procmail"
```

(oui, c'est tout)

Maintenant, tous les messages qui vous sont envoyés passent par spamassassin, dont vous pourrez modifier la config qui se trouve dans le répertoire `/etc/spamassassin`, afin de l'assaisonner à vos besoins (pour le moment ça me convient tel que).

Au final

Pourquoi avoir choisi Spamassassin ?
Parce que son système de notation du spam permet de régler très finement ce qu'on considère comme étant du spam, et, qu'à priori, les fichiers de config sont relativement faciles à lire.

Voici le résultat d'un mail filtré avec Spamassassin :

```
SPAM: -------------------- Start SpamAssassin results  SPAM: FROM_NAME_NO_SPACES (-0.1 points) From: no spaces in name SPAM: MSG_ID_ADDED_BY_MTA (4.0 points)  'Message-Id' was added by a relay SPAM: KOREAN_UCE_SUBJECT (3.4 points)  Subject: contains Korean unsolicited email tag SPAM: INVALID_MSGID (1.8 points)  Message-Id is not valid, according to RFC-2822 SPAM: NO_REAL_NAME       (0.5 points)  From: does not include a real name SPAM: FROM_ENDS_IN_NUMS  (0.4 points)  From: ends in numbers SPAM: PLING      (0.1 points)  Subject has an exclamation mark SPAM: MAILTO_TO_SPAM_ADDR (0.5 points)  URI: Includes a link to a likely spammer email address SPAM: MAILTO_LINK        (0.8 points)  BODY: Includes a URL link to send an email SPAM: SUBJ_FULL_OF_8BITS (4.3 points)  Subject is full of 8-bit characters SPAM: DATE_IN_PAST_12_24 (1.7 points)  Date: is 12 to 24 hours before Received: date SPAM: CTYPE_JUST_HTML    (1.7 points)  HTML-only mail, with no text version
```

On voit ci-dessus que Spamassassin note chaque *composant type* d'un mail de spam, et détermine de la sorte si le mail peut être considéré comme étant du spam.

Post-scriptum :

– SPAMassassin
– Sendmail, ou sur le site CLX
– Procmail
– Des articles sur le fonctionnement général d'une messagerie et sur SPAMassassin http://www.troubleshooters.com/lpm/...

Copyright © Club LinuX Nord-Pas de Calais